DEPARTMENT OF HOMELAND SECURITY

- - -

MEETING OF THE

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

TELECONFERENCE

- - -

Thursday, May 19, 2011
Ninth Floor Conference Room
1621 North Kent Street
Rosslyn, Virginia

The meeting was convened, pursuant to notice, at 11:02 a.m., RICHARD V. PURCELL, Chairman, presiding, and was reported from 1621 North Kent Street, Rosslyn, Virginia.

COMMITTEE MEMBERS PARTICIPATING: (By telephone)

RICHARD V. PURCELL, Chairman, presiding

ANA I. ANTON
RAMON BARQUIN
J. HOWARD BEALES III
DANIEL W. CAPRIO, JR.
DAVID A. HOFFMAN
LANCE HOFFMAN
JOANNE McNABB
NEVILLE PATTINSON

LAWRENCE PONEMON JOHN SABO
LISA J. SOTTO

ALSO PRESENT:

MARTHA K. LANDESBERG, Executive Director
and Designated Federal Official

P R O C E E D I N G S

MS. LANDESBERG: We'll go on the record. I am Martha Landesberg, the Designated Federal Official for the DHS Data Privacy and Integrity Advisory Committee meeting. I welcome you all, and I would like to take a moment to ask whether members of the public other than the committee members have joined us this morning, and if so if you care to identify yourselves?

MR. STEINHART: Yes, this is Barry Steinhart.

MS. LANDESBERG: Good morning, Barry.

MR. STEINHART: Good morning.

MR. NOJEIM: Greg Nojeim from CDT.

MS. LANDESBERG: Good morning. Thank you.

MS. LANE: Kamala Lane, Washington Internet Daily.

MS. LANDESBERG: Thank you, Ms. Lane.

All right. With that, you're more than welcome to join us. We're glad you're here, and with that I will turn the meeting over to the Chairman, Richard Purcell.

CHAIRMAN PURCELL: Thank you, Martha.

Welcome to the DPIAC meeting. The first thing, because this is a teleconference, we'll ask all

participants to the meeting to please mute your phone while listening. Keep in mind that if you want to speak that your phone will be muted and you'll have to unmute it.

We've reserved time at the end of this teleconference from 12:30 to 1:00 p.m. for public comment. If there's anyone on the phone now who wishes to address the committee later this morning, please state your name and that intention. If you're not certain about whether you want to address the committee now, I will ask you again later before the public comment begins. But I will be taking those calls in order, so please state your name and affiliation --

MS. HOLLIDAY McDONALD: Melinda Holliday McDonald, DHS OIG.

CHAIRMAN PURCELL: Thank you. What's that name again?

MS. McDONALD: Melinda Holliday McDonald, with DHS OIG.

MS. CALLAHAN: Melinda, I don't know if you were intending to address the committee or if you were just RSVPing. If it's the latter, that's okay. We don't need

to have each individual RSVP on this call.

MS. HOLLIDAY McDONALD: Just RSVPing, thanks.

MS. CALLAHAN: Great.

CHAIRMAN PURCELL: So again, if anybody wants to address the committee, if members of the public want to address the committee, please state your name and affiliation now and I will call on you in order of that at the end of the meeting. We'll ask that those comments be limited to approximately 3 minutes.

Are there any individuals wishing to address the committee at this time?

(No response.)

CHAIRMAN PURCELL: No. As I said, I will take that opportunity to request names for that purpose throughout the meeting.

All the speakers, including the committee members: It's going to be important, because this is a teleconference, to state your name each time you speak. This will not only assist us to understand who's speaking, but it'll also help the court reporter prepare an accurate transcript of the day's proceedings. So please, mute phones if you would, please, to prevent background noise

from interrupting and interfering.

At this time I'd like to turn to Mary Ellen Callahan, the Chief Privacy Officer of the Department of Homeland Security. Prior to joining the Department of Homeland Security, Ms. Callahan specialized in privacy, data security, and consumer protection law as a partner of Hogan and Hartson, LLP, in Washington. Mary Ellen has served as Co-Chair during that period of the Online Privacy Alliance, an industry self-regulatory group, and as Vice Chair of the American Bar Association Antitrust Division Privacy and Information Security Committee.

Together with the DHS Privacy Office team, Ms. Callahan is responsible for privacy compliance across the Department and all its components. She also serves as the Department's Chief Freedom of Information Officer.

It's been a really busy couple of months for Ms. Callahan and the Privacy Office since we met last and we're eager to hear about what the last few months has entailed. Mary Ellen, please proceed.

DHS PRIVACY OFFICE UPDATE,

BY MARY ELLEN CALLAHAN

MS. CALLAHAN: Thank you very much, Mr.

Chairman, and welcome to all of those on the call.

First, I'd like to note that this is a relatively novel approach for us to host a DPIAC Committee meeting, and so I ask everybody's indulgence. We may have a few glitches, we may have a few stumbles, but we are happy to provide this public information pursuant to the FACA Act as well as to our requirements as DPIAC.

So again, just to repeat Richard's comment, if you guys can put your phones on mute that would be very useful.

So first I want to begin the meeting with an overview of the activities since our last meeting in early March. As Richard indicated, the office has been quite busy. Following my report, Christopher Lee, the Privacy Officer of the Department's Science and Technology Directorate, will brief you on how privacy is being incorporated into S&T's work. Chris's presentation is the fourth in our series of briefings for the committee by DHS component privacy officers, and it was specifically an outgrowth of things that we discussed at our last meeting.

I want to thank Chris for joining us today and I know that you're going to look forward to hearing from him

and all of his strong work that he's been doing since he became the S&T privacy officer approximately 7 months ago.

As always, I have many exciting developments in the Privacy Office and throughout the Department of Homeland Security to report. First, I am pleased to tell you about two new important additions to the DHS privacy team, or family, as we like to think of it. In March Delores Barber joined us as our new Deputy Chief FOIA Officer. Delores brings with her 20 years of federal management and IT experience to this position. Prior to joining the Department of Homeland Security, she served as the Department of Education's FOIA Officer and also served as the Director of the Department of Education's FOIA Service Center and Acting Director of its $1 billion IMPACT Aid Program. Delores has been a great addition already and we'll talk about some of her initiatives as I give the presentation.

Then in April Jordan Gottfried came on board as our first Chief of Staff. Jordan has served in various capacities during his 5 years in the Department, most recently as the Chief of Special Programs in the Headquarters Office of Operations. He also served as the

Director of Response Policy while on detail to the White House National Security Staff. Jordan will leave our -- will lead our administrative team.

I hope you will join me in welcoming Jordan and Delores. They are great additions to our leadership team, and with them that rounds out the expansion of the DHS Privacy Office. As noted in the last meeting, we have added 23 positions in my 2-plus years in the Department, 18 of which were derived from converting contracts that we've done in the Department. So we've got what I consider to be an insurmountable team here, and I want to thank everyone and welcome Delores and Jordan and look forward to their strategic vision.

The first thing to discuss is information sharing. Our new Privacy Information Sharing and Intelligence Group has quickly come together on a number of important initiatives. As you may recall from our last meeting, Howard Schmidt announced the national -- announced that the National Strategy for Trusted Identities in Cyberspace, or NSTIC, was close to being signed. The document was signed on April 15th and I'm pleased to say that the DHS Privacy Office senior staff

provided privacy expertise and served on the core writing team for the final strategy. PRIVTECH staff will continue to provide privacy subject matter expertise to the NSTIC program office, now located in NIST at the Department of Commerce, to support implementation of the strategy as necessary.

We will also continue to provide intensive privacy support -- we also continue to provide intensive privacy support for state and local fusion centers. You will recall that the continuing use of DHS grant funding was tied last year to the requirement that all fusion centers have a written privacy policy that is at least as comprehensive as the federal information-sharing environment privacy guidelines.

I'm happy to report that our efforts to review fusion center privacy policies are completed. All 71 designated fusion centers now have privacy policies that meet the standard and have done so as of March 2011. We discussed at the last meeting that we were almost there and indeed we did meet that goal.

I believe that all centers make their policies available upon request. A sizable majority have posted

their policies on the National Fusion Center Association's website, which is www.nfcusa.org. That's National Fusion Center usa.org. And more are doing so every day at our encouragement.

One center has not yet been formally established by its governor and we anticipate that that center will submit its policy for review once it's formally established by the governor, and we anticipate that that will be soon.

We also continue to review any policy that's sent to us by a fusion center node, i.e., a regional center that has a relationship to one of the 71 or 72 designated centers. So far we've seen about ten of these and could see as many as a dozen more. So we continue to be involved in the development of privacy policies for fusion centers.

Now that our attention is turning to what we can do to help fusion centers build and mature their privacy protection infrastructure, this begins with training. A few meetings ago I described our three-pronged training program, which continues apace even in this difficult budget environment. Last week Privacy Office staff

traveled with counterparts from CRCL to Ohio to conduct training for three different fusion centers that had assembled in one venue. Upcoming trips are also planned for Tennessee and Chicago.

This summer we're planning to hold another train-the-trainer session where DHS invites fusion center privacy officers to Washington to hear how we train on privacy and civil liberties issues and for assistance on designing their own training on state law requirements and fusion center practices.

As you recall, we hosted several regional train-the-trainer events when training all 72 privacy and civil liberties officers last year. This proposed meeting is to provide further training for new officers and supplemental training for ongoing officers.

Now that the privacy policy review process is complete, we can also focus on conducting the second of two Privacy Impact Assessments required by the 9-11 Commission Act. The first was published in December of 2008 and this PIA -- this upcoming PIA will provide an update on the state of the program and address additional steps the Department and individual fusion centers can

take to protect privacy while they conduct their important counterterrorism mission.

In addition, when approving the privacy policies for the fusion centers we encouraged the fusion centers to do their own Privacy Impact Assessment on the center or on the program or databases as appropriate, and several are in the process of doing so right now.

In addition to these important state and local initiatives, the group continues to review homeland intelligence reports and intelligence products written by the Department's Office of Intelligence Analysis. Since the last DPIAC meeting my team has reviewed 69 HIRs and 55 intelligence products. The intelligence team is accomplishing this task quickly, with the average time from receipt to response continuing to decrease well below the required 48-hour response time.

As you know, we address international privacy issues on many fronts. We remain actively engaged in the continuing negotiations for a U.S.-European Union passenger name records, or PNR, agreement. The negotiations for the Department are being led by the Deputy Secretary. I returned Tuesday night from our most

recent round of negotiations with the European Commission. We have made considerable progress and are close to reaching an agreement with the European Commission.

Furthermore, negotiations are also under way for a U.S.-EU umbrella data protection and privacy agreement that would provide a framework for mutual recognition of our privacy systems to facilitate the exchange of law enforcement information between governments. Deputy Chief Privacy Officer John Kropf, IPP Director Lauren Saadat and I have been serving on the negotiating team as privacy subject matter experts, both in inter-agency planning sessions and in negotiating sessions with the EU.

Together with the Federal Law Enforcement Training Center and Office of International Affairs, IPP Director Shannon Ballard is developing privacy training programs for DHS personnel stationed overseas as part of a broader pre-deployment training. Shannon is also working with the Department of State to include a data privacy policy course for other U.S. Government overseas personnel, to be held at the Foreign Service Institute.

The goal here is to provide a general understanding of the U.S. privacy framework and to raise awareness of

privacy as a foreign policy issue relevant to a number of U.S. Government objectives.

One of the Department's major international initiatives is increased cooperation on migration and border system in the Five-Country Conference, which includes New Zealand, Australia, the U.K., Canada, and the U.S. My international and information-sharing teams coordinate with the DHS Office of Policy on this initiative as it pertains to new information-sharing programs.

IPP continues to provide subject matter expertise to the DHS negotiating team that's undertaking numerous preventing and combatting serious crimes agreements, as required to be signed with visa waiver program member countries. I expect to soon release with my DOJ counterpart a privacy policy memorandum that describes the privacy protections statutorily required in PCSC agreements. This memorandum will set a standard that will help ensure consistency of privacy protections throughout the PCSC agreement, encourage adoption of reciprocal protections by our international partners, and set the standard for transparency on these issues.

Lauren Saadat also coordinated joint DHS-DOJ-State comments on the Council of Europe's consultation on the modernization of Convention 108, which has served as the backbone of international privacy law for over 40 countries. The U.S. Government comments are available on the Council of Europe web site.

Speaking of outreach, as you know, my office engages in a great deal of outreach, both international and domestic. Here are a few highlights: On April 13, I gave the keynote address at the European Institute's roundtable discussion on homeland security with members of the European Parliament's Civil Liberties, Justice, and Home Affairs Committee, also known as the LIBE Committee. The keynote address was entitled "Strengthening Civil Liberties and Security: EU-U.S. Cooperation on Data Protection, Privacy, and SWIFT."

On Tuesday this week, together with the DHS General Counsel and Customs and Border Protection, I spoke to a sell-out crowd in Brussels on the use of PNR by DHS and the privacy protections therein.

Earlier this month I attended the Biometrics and Security in Global Perspective Conference, where I

represented the office as a keynote speaker. The conference was organized by the Center for Policy on Emergent Technologies and it's part of the rising pan-European and international awareness on biometrics and security ethics project.

Debbi Diener, Director of Privacy Policy, was a discussant for the panel for five presentations on different aspects of biometrics. She discussed the privacy implications raised by biometrics and responded to the panel topics, which included emerging biometric technologies, the use of facial recognition, medical health issues, and the use of biometrics Privacy Impact Assessments.

I know the committee is well aware of the role our compliance team has in ensuring that the Department's programs and systems adhere to law and DHS privacy policy. Since the last DPIAC meeting, the compliance team has published nine Privacy Impact Assessments and eight SORNs. Therefore, the DHS FISMA score remains at 72 percent for PIAs and 92 percent for SORNs.

Programs for which documentation was approved and published on the DHS privacy web site,

www.dhs.gov/privacy, they include the DHS Sharepoint and collaboration sites, DHS integrated security management system, the DHS management directives foreign national visitors management system, and the National Protection and Programs Directorate's critical infrastructure warning information program. So I encourage all to take a look at that information.

Our policy group continues to work to embed privacy in DHS programs and its inter-agency efforts. In her role as Co-Chair of the Identity Management Subcommittee of the CIO Council Privacy Committee, of which of course I'm a co-chair of the committee, Debbi Diener is actively engaged with a broad range of inter-agency activities for the Federal Identity Credential and Access road map and implementation guide, the FICAM road map, as it's colloquially known. The subcommittee collaborates with federal IT and security staff on the road map development team, where their input serves to ensure that privacy requirements and protections and guidance are included in the implementation chapters for the FICAM road map, and that should be a very useful tool, not just for the federal community, but for identity

management overall.

Here in the office, we've begun our work on our 2011 annual report to Congress. As you know, this report showcases not only my office's activities, but those of the DHS component privacy offices, as we work together to operationalize privacy throughout the Department. The theme for this year's annual report is "How we make a difference," basically what do we do that supports the Department throughout the process.

Our Privacy and Technology Group continues to develop policies to address privacy issues raised by the Department's use of various technologies. They also continue to be involved in the Federal CIO Council's process know as FEDRAMP, the Federal Risk and Authorization Management Program, to ensure privacy is considered throughout the planning and implementation of cloud computing in the Federal Government. Additionally, the PRIVTECH team has participated in a number of tiger teams regarding privacy and cloud computing.

Privacy technology, together with the privacy compliance and the NPPD privacy officer, is currently preparing a Privacy Impact Assessment for Einstein 3, the

intrusion prevention system the Department is deploying pursuant to Initiative 3 of the Federal Government's comprehensive national security -- national cyber security initiative.

And Pete Sand, our Director of Privacy Technology, continues to staff the Department's Office of Cyber Security Coordination, located at the National Security Agency, along with DHS Office of Civil Rights and Civil Liberties and the Office of General Counsel members as well. We discussed that at our last meeting.

(Music from the phone line.)

MS. CALLAHAN: If everyone could put their phone on mute, please, or if they are on hold we may have a problem. But, oh well.

I appear to have some fabulous music going on. Just one moment.

I will periodically remind those to not put us on hold if indeed they have music. Hopefully, you will be able to continue to hear, and I look at the court reporter and he is fine. So we will go on.

I mentioned the addition of Delores Barber as the first ever Deputy Chief FOIA Officer. Our FOIA work

continues apace under her leadership. At this time last year, the Department overall had received 73,213 FOIA requests, on our way to receiving 133,000 FOIA requests. This year we have received 89,788 requests to date for this fiscal year, an increase of a little over 22 percent over last year.

We continue to move apace and to make sure that we are able to meet our statutory FOIA responsibilities despite receiving -- last year we received 24 percent of all FOIAs that the entire Federal Government received, and we will likely exceed that percentage and exceed 130,000 FOIA requests for this year as well. But I want to thank all the FOIA officers in the components for working diligently to make sure that we indeed not only are able to reduce the backlog, but are able to meet our open government responsibilities and projects.

In fact, I point to our FY 2011 DHS Chief FOIA Officer report, which was released on March 29, 2011. I encourage the committee and the public to take a look at that report. That can also be found on our web site. There's also a specific dhs.gov/foia web site, where the report and several other elements are to be found, where

we go into detail about what we've done to continue to support transparency and open government.

We take a very aggressive approach to proactively disclosing information, in keeping with the President's open government directive and related transparency initiatives. Not only is that detailed in the Chief FOIA Officer report, but, consistent with my proactive disclosure policy memorandum in 2009, during this reporting period DHS has published more than 69 documents totaling 9,132 pages -- a 46 percent increase in the total numbers of pages published in our last reporting period.

So we will continue to work to proactively disclose more frequently requested and important policy documents. Relatedly, we are continuing to post FOIA logs for each DHS component beginning with the January 2009 records and continuing to the present fiscal year. I actually noticed yesterday that we are perhaps not fully up to date on some of those, and I'll be reaching out to the component FOIA officers to make sure that we present a consistent proactive disclosure for our FOIA logs, because these logs provide valuable insight into the type of

information sought by the public through the FOIA request process and also make them useful tools in understanding what DHS operations are of particular public interest and allow us to identify the types of information that we should be disclosing proactively. So we'll hear more about that likely in July.

Then finally, for incidents and inquiries we've had quite a busy time, but in addition on May 4 Rose Bird, Director of Privacy Incidents and Inquiries, and her staff hosted the second Privacy Incident Handling Quarterly Meeting and presented an overview of privacy incidents at DHS from January through March 2011. Participants included, as always, component privacy officers, privacy points of contact, DHS enterprise operations staff, who shared information on privacy incident managing and mitigation and on incident prevention. We are working to really systematize and coordinate our incident prevention and management systems on several levels.

(Music from the phone line.)

With that said, despite the music, I am going to turn it back over to the Chairman, Mr. Purcell. That concludes my report to the committee.

CHAIRMAN PURCELL: Thank you, Mary Ellen.

I hope that individuals can hear me. If there are any committee members who have joined following the roll call that was taken at the beginning of the teleconference, could you identify yourself at this time?

MR. CAPRIO: Dan Caprio.

CHAIRMAN PURCELL: Dan Caprio.

MS. ANTON: Annie Anton.

CHAIRMAN PURCELL: Annie Anton.

MR. SABO: John Sabo.

CHAIRMAN PURCELL: John Sabo.

Ms. McNABB: Joanne McNabb.

CHAIRMAN PURCELL: Joanne McNabb.

Okay, that's great. If any committee members would like to respond to or have a question of Ms. Callahan, please let me know if you do and I will do my best to call upon you in a reasonable order here. Are there any questions from the committee members?

(No response.)

VOICE: Richard, can we cut off the line of the person who we have on hold?

CHAIRMAN PURCELL: I don't think so.

MS. CALLAHAN: Charlie is looking into whether or not we can do that. Again, my apologies for this. This was a relatively novel approach and we have identified areas we can improve.

VOICE: Well, if we all hang up and dial back in?

MS. CALLAHAN: No, because they'll still be on, because they won't know it. So I think we just kind of bear with it. It's not as though my voice is not heard.

Actually, maybe, Richard, I would suggest when we don't hear the music we may want to repeat that whoever was on hold had put us on hold.

CHAIRMAN PURCELL: Yes, that's my intention.

MS. CALLAHAN: Thank you.

CHAIRMAN PURCELL: So, with a back beat here, Charlie, if you could just send out a message to all --

(Music on phone line stops.)

CHAIRMAN PURCELL: Oh, there we go. Somebody's gotten off hold.

One of the important things about this call is that if there is a -- if any of the participants put a call on hold and they have music in the background, that

music plays for everybody. Sharing is good, but sharing is not caring in this situation. Do not put this call on hold. If you have to put it on hold, close the call and call back in when you've concluded your other business.

Again, if any committee members have questions for Ms. Callahan, please let me know now.

(No response.)

CHAIRMAN PURCELL: Hearing none, I will remind any members of the public who are on the call that if they have an opportunity -- that they do have an opportunity at the end of the call to make comments. If there are members of the public who would like to make comments, I would like to have them identify themselves now, please, so I can put you on a list for that period.

Hearing none, I'll turn to our next speaker, who is Mr. Christopher S. Lee, the Directorate Privacy Officer for the DHS Science and Technology Directorate. Mr. Lee assumed this position in November and his responsibilities include managing privacy compliance requirements and implementing privacy best practices in the science and technology programs and projects.

Prior to joining S&T, Mr. Lee spent 2 years

working in the U.S. VISIT Privacy Office in the DHS National Protection and Programs Directorate. At that time he was focused on enforcing privacy protections for the Automated Biometric Identification System, also known as IDENT, the world's largest biometric database.

He's also worked in the Government Accountability Office as a contractor, helping to stand up the GAO Privacy Office for the first time, and has also served as the United States Senate's first webmaster.

Mr. Lee is joining us today to provide the committee an update on the S&T implememententations of DHS privacy policies. Mr. Lee, welcome. Please proceed.

DHS SCIENCE AND TECHNOLOGY DIRECTORATE'S IMPLEMENTATION OF DHS PRIVACY POLICY,

BY CHRISTOPHER S. LEE

MR. LEE: Good morning, Chairman Purcell, members of the committee, and Chief Privacy Officer Callahan. Thank you for inviting me to address the committee today. I'm honored to be here. I realize for many of you the only thing that stands between lunch and having lunch is this presentation. Therefore I will attempt to move along at a reasonable pace.

So, moving right along: The Department of Homeland Security Science and Technology Directorate, or "S&T," is known for providing its customers with state-of-the-art technology that helps them achieve their missions. In my presentation today, I will discuss Science and Technology's recent organization, its authority, the S&T Privacy office, and my efforts to integrate privacy into the Science and Technology Directorate.

The Science and Technology Directorate was established by the Homeland Security Act of 2002, Public Law 107-296, Title III. Dr. Tara O'Toole is the Under Secretary for Science and Technology and Mr. Paul Benda is the Acting Deputy Under Secretary.

The S&T Directorate reorganized on November 2010 and the Science and Technology Privacy Office was reassigned from the Office of Regulatory Compliance and now reports directly to the Office of the Under Secretary. This reporting structure gives the Science and Technology Privacy Office a very high level of visibility.

S&T's authority includes advising the DHS Secretary regarding research and development issues, developing a national plan to identify and develop

countermeasures to chemical, biological, and other emerging terrorist threats, and conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department for both intramural and extramural programs.

The "intramural" refers to DHS's internal support components, such as Customs and Border Protection, Immigration and Customs Enforcement, and Citizenship and Immigration Services. And "extramural" refers to supporting organizations outside of DHS, such as state and local first responders and law enforcement agencies.

The Science and Technology Directorate manages, oversees, or conducts more than 120 projects, ranging in areas such as border and maritime security, chemical and biological defense, cyber security, explosives, human factors and behavioral sciences, and infrastructure protection and disaster management.

As the Chairman mentioned earlier, I was brought on board to the Science and Technology Directorate in November 2010 as the Directorate's first government privacy officer. Prior to joining S&T, I was at the U.S.

VISIT program as the Deputy Privacy Officer under Paul Hasson, U.S. VISIT's Privacy Officer, and I'd like to take a moment to thank Paul for his leadership and guidance while I was at U.S. VISIT.

The S&T Privacy Office was established in 2007. Contractors have been assigned to the directorate privacy office since its inception. The initial responsibilities of the office included privacy compliance, training, consulting, responding to and mitigating privacy incidents, and collaborating with the DHS Privacy Office to develop privacy principles that guide the research and development process.

Two contractors are currently assigned to the S&T Privacy Office. Kathryn Fong, Senior Privacy Analyst, has been with the S&T Privacy Office for 3 years; and Jaeme Drake, Privacy Analyst, has been with the Privacy Office for 2-1/2 years. I'd like to take a moment here and thank Kathryn and Jaeme for their dedication and efforts in supporting the S&T Privacy Office.

When I first started at the directorate in November 2010, I established three goals to achieve in the first 90 days: Number one, individually meet with the

directorate's senior staff and division heads; number two, review existing privacy policies, processes, and procedures and identify gaps or opportunities to streamline work; and number three, maintain existing privacy compliance requirements.

In that 90-day time frame, I met with the majority of the directorate's senior staff and division heads, and in those meetings I explained to the senior staff and division heads my privacy philosophy. That philosophy is based largely on the privacy by design concepts. Two specific privacy by design objectives I stressed in my meetings are: number one, embedding and integrating privacy into the life cycle of projects, including early integration during the initial concept phase; and number two, creating a win-win situation where program managers can achieve their project goals and at the same time respect individual privacy rights.

This approach helps Science and Technology program managers view the Privacy Office as an integral partner in the project life cycle, instead of looking at the Privacy Office as an insurmountable obstacle to achieving their project goals. Program managers now

recognize that the Directorate Privacy Office shares a common goal of identifying, researching, testing, and evaluating products and services that support and protect the homeland. This approach has led to program managers to actively seek me and my office out for privacy consultations early on in the project concept and initiation phases.

In my review of existing privacy policies, Kathryn Fong and Jaeme Drake brought to my attention an opportunity to write an umbrella Privacy Impact Assessment for volunteers participating in S&T-sponsored research projects. S&T works with volunteers to help test, evaluate, and provide feedback on technologies and equipment. For example, S&T will work with firemen who volunteer to test new or enhanced fire equipment, such as new oxygen tank designs or boots that are more water-resistant and heat-resistant than existing equipment.

In each of these studies, S&T collects a limited amount of personal information from the volunteers and upon completion of the study all volunteer data containing PII is destroyed. Previously, a new PIA was required for each study. But with the introduction of the volunteer's

PIA, the majority of S&T's basic research studies involving volunteers are now covered under this umbrella PIA. This saves both time and money for DHS.

In the 7 months I have worked at S&T, my office has written or worked on five Privacy Impact Assessments, written, edited or reviewed 33 privacy threshold analyses, retired five Privacy Impact Assessments because the projects had finished, retired 20 privacy threshold analyses, again because the projects had finished, reviewed and updated three system of records notices, and conducted a privacy presentation at the S&T Directorate all-hands meeting attended by 300 staff.

Understanding the difference between S&T and DHS's operational components is key to understanding what the privacy risks each organization faces. S&T is a research organization. It does not have uniformed officers or officers who carry weapons or any authority to make arrests. Contrast that to DHS operational components such as Customs and Border Protection, Immigration and Customs Enforcement, the Coast Guard, and the Secret Service. These operational components have so-called "boots on the ground." They have uniformed officers who

carry weapons and have authority to make arrests.

S&T's research mission differs from these DHS operational boots on the ground components because S&T conducts feasibility studies that focus on the essential question, does the technology work, whereas operational components deploy technologies that have been fully tested and are known to work and ask, how can I make this work best in an operational setting?

Looking at as a two-phased process, in phase one S&T privacy focuses on laboratory and field test privacy risks and in phase two operational component privacy offices, such as CBP, ICE, and TSA focus on privacy risks, policies, and procedures that arise as products and technologies are transitioned and operationalized.

Frequently, the public, the media, or civil liberties groups hear about Science and Technology projects that potentially impact individual privacy and immediately begin asking questions about operational privacy risks, policies, and procedures. The S&T Privacy Office can address phase one laboratory and field test privacy risks and steps taken to mitigate those risks. Then the S&T Privacy Office works with the operational

component privacy officers to identify and recommend mitigation strategies for phase two operational privacy risks, policies, and procedures.

The final privacy policies and procedures for transitioned and operationalized technologies are determined by the operational component in conjunction with the DHS Privacy Office and with guidance provided by my S&T Privacy Office.

So, looking at a couple of examples, one is the Border Patrol communications radio project. This is an initial stage project, that is gathering requirements to purchase new communications radios for Border Patrol officers. Border Patrol officers frequently work alone in long stretches of uninhabited terrain. Officer safety is of paramount concern because Border Patrol officers have been victims of weapons and drug smugglers. S&T is working with the Border Patrol to identify those radio requirements and S&T will conduct laboratory and field tests for those radios.

One of the requirements is to include a GPS location device that can be activated to identify the location of a Border Patrol officer who may be in danger.

Volunteers participating in lab or field tests will be notified about the GPS locator device in the radios and will be asked to give consent to using and testing the GPS device. This notice and consent during the testing process addresses the primary risks that S&T Privacy is looking into.

After the communications radios are deployed and operationalized for Border Patrol officer use, the operational privacy policies and procedures will need to be addressed. The biggest issue is that the government may end up tracking all movements of Border Patrol officers.

So the S&T Privacy Office recommends the following mitigation strategies: Number one, identify that officer safety is the primary reason for the GPS locator; two, the GPS locator is only activated if the supervisor has reason to believe that the officer's safety is in question; three, officers are provided notice of the GPS locator in the radios and procedures on when the GPS locator device is activated; and also identify that the radio containing the GPS locator is government-purchased and furnished equipment, not personal property owned by

the individual officer.

These privacy risk mitigation strategies will help assure that officer safety is ensured and at the same time officer privacy is respected.

Ultimately, the GPS locator usage policies will be determined by the component, and in this case that means the Customs and Border Protection, Border Patrol office will establish the operational policies and procedures. My office will work with CPB's Privacy Office to recommend mitigation strategies that respect individual privacy rights.

This is also one example of where the Science and Technology program manager working on the communications radio project actively sought out the advice of the S&T Privacy Office early in the project, and it's an example of the differences between the S&T privacy issues as opposed to the operational component privacy issues.

Another project that we're working on is called the CELL ALL project. "CELL" is spelled C-E-L-L as in "cell phone." CELL ALL is a personal environmental threat detector system that is currently under development by a

third party contractor. The system consists of multiple sensors which are miniaturized into a device and attached to an individual's cell phone. In the event of a chemical spill, the CELL ALL unit identifies the type of chemical and then transmits that information along with location information to a computer server. The server will then transmit that information to the proper authorities, such as a HAZMAT team or first responders.

Identifying the privacy risks, they fall into two categories, transparency and geolocation concerns. In terms of transparency, with user consents provided to the individual testers each user consents to some information being transmitted, but for the test phase that S&T is conducting no PII is used, captured, or transmitted.

In terms of the geolocation information concerns, the location information is transmitted, but again with the user consent, and again no associated PII is sent with the user location information. Further, users participating in the test may turn off their cell phone and stop participating in this test at any time.

A fair information practice principles PIA was conducted to cover the demonstration portion of this

project. Once the development and testing are complete and S&T validates the technology, it will be transitioned to the private sector and marketed by commercial vendors.

In addition to my existing responsibilities as the directorate's privacy officer, I am focusing on creating an information life cycle management office. The concept is to create a one-stop, cradle-to-grave information and data management advisory office. The S&T information life cycle office will consist of the Privacy Office, the Freedom of Information Act Office, records management, and Paperwork Reduction Act work.

S&T program managers can come to the information life cycle management office and obtain guidance on research data that may or may not contain PII, and they can ask questions such as: What are the data and information compliance requirements? What data can be shared? When can the data be shared? What agencies can the data be shared with? What can be disclosed and when should data be destroyed or archived?

The goal of the information life cycle management office is to help streamline information and data management processes at the Science and Technology

Directorate.

In closing, I'd like to say that as the directorate's first privacy officer I look forward to using state-of-the-art privacy and information management principles to help S&T fulfil its mission.

Chairman Purcell and members of the committee, I thank you for your time and I'm now happy to address any questions you may have.

CHAIRMAN PURCELL: Thank you, Mr. Lee. I appreciate your comments. I wanted to -- I'll ask the committee members for questions. I wanted to first pose the question, Mr. Lee, about the concept of privacy by design and how you incorporate that into your S&T projects and how you may communicate that to the component groups that are essentially customers of your services?

MR. LEE: So the question was how privacy by design is incorporated in projects and how notification is sent out to staff.

CHAIRMAN PURCELL: Yes.

MR. LEE: In regard to privacy by design, one of biggest surprises I've found out is that there is no specific system development life cycle management process

within S&T. They use several different models, but within the models there are usually opportunities to incorporate various compliance requirements, such as privacy issues, in those models. And S&T is moving toward adopting a larger, catch-all model of system development, life cycle design, but it's an iterative process and we're going around in that process.

In terms of notifying staff as to about the various privacy by design requirements, it's been done in a number of different ways. One is for a direct outreach with the different divisions, the division heads and the different staffs. Another is through staff meetings that we've had, such as the all-hands meetings, where usually 2 to 300 staff attend. Another is through standard training, where we have an internal training program and we let staff -- the internal training is required on an annual basis, and in that training we let staff know that they should approach the Privacy Office if there are any issues pertaining to PIA or privacy that need to be addressed.

CHAIRMAN PURCELL: Excellent. Thank you for that.

Are there any committee members who have questions for Mr. Lee? Please, if you do, let me know and I will do my best to call upon you in order.

MR. SABO: John Sabo.

CHAIRMAN PURCELL: Okay, John. Anybody else?

(No response.)

CHAIRMAN PURCELL: John, what's your question?

MR. SABO: Mr. Lee, thanks for your speaking with the committee today. My question goes a little bit to, in your role clearly you're addressing privacy in the S&T organization and all the programs operated by S&T. I'm wondering, as privacy officer if you get engaged at all in the research proposals that S&T funds that may impact on privacy as an actual research project, not the privacy impact of the project on individual privacy, but the potential for research that might help DHS manage privacy in many of its components.

It may be that's not in your portfolio, but I was just wondering if you get into that type of role as privacy officer.

MR. LEE: Regarding the question about research proposals for specific privacy development opportunities,

in my office and within S&T that isn't one of the areas that's covered, although it would be an area I'd personally like to pursue. Unfortunately, my management has different direction opportunities that they're pursuing at this moment.

MS. CALLAHAN: Chairman Purcell, maybe I can ask a question to my colleague Mr. Lee?

CHAIRMAN PURCELL: Yes, please.

MS. CALLAHAN: So you talked a little bit about working with the Customs and Border Protection operational component privacy officer. How is that working out and do you envision continued collaboration as Science and Technology develops programs on behalf of, as you said, kind of the internal clients that you described?

MR. LEE: My work with CBP and other components' privacy officers has actually been quite good. In my time at U.S. VISIT, I had an opportunity to meet and work with a number of the government privacy officers, so I have a good working relationship with them. What I am able to do is just pick up the phone and contact them directly when any projects come up and when any potential risks come up, both on the research side and the operational side. So I

can give them a very clean and clear heads-up as to what's happening on my end and then what will be coming down the road on their end as the project becomes operationalized.

By and large, the partnership has been working quite well.

MS. CALLAHAN: Great. If I can, Mr. Chairman, as well as for the committee members, part of that, part of having Chris and his success so far in the process, has been, as you know, about 2 years ago the Deputy Secretary directed that all the components, operational components, have privacy officers. About half did at the time. Then we also had the Directorate of Science and Technology, the Directorate of National Protection and Prevention Directorate -- so I had two "D's" there -- and the Office of Intelligence and Analysis. Three right now non-operational components have privacy officers to try to make sure that we do capture the life cycle of privacy projects and to make sure that indeed from research to analysis to implementation that the privacy protections are considered throughout.

So I would just thank Chris for his work and posit that this has been a real success story to make sure

that we are capturing the whole spectrum of DHS's work with privacy-sensitive technology and programs as a result.

CHAIRMAN PURCELL: Thank you, Mary Ellen.

Joanne, do you have a question?

Ms. McNABB: Yes. I'm mute.

I was interested in what you had to say about the distinction between the phase one privacy issues in project development and then the phase two issues in field implementation. I'd be interested in hearing a little more about how that transition works and how you address -- to what extent you address phase two.

MR. LEE: In regard to phase one privacy, my office looks at the privacy issues that S&T has direct control over, which is usually testing within the laboratory or basic field test research. After that, after the product or technology has been fully tested and transferred over to the operational component, the phase two portion, usually what happens is I work with the component privacy officer and I let them know what privacy concerns we've identified in the broader scope, not just within the laboratory test, but what the broader

operational issues will be, and I'll give them guidance on what the conditions on how to set up the operational privacy policies would be.

But it is just guidance, because each component has its own rules and guidelines. Since I don't work specifically with people, those boots on the ground, I don't know exactly what they're going through on a day to day basis. But the privacy offices in those operational components have a better idea and have a better understanding of the different customer service aspects, the different criminal issues that are coming up, and how to best implement the privacy practices into that phase two operational setting.

Ms. McNABB: Do you surface the operational privacy implications that you're aware of in your PIA?

MR. LEE: In the S&T portion, usually I do not address those issues, because the technology may or may not work beyond the laboratory. So what we try to do is focus on the laboratory and initial test phase.

In a lot of research, we find out that the technology is not working the way the vendor has proposed it will work. So it doesn't get beyond the operational --

the test phase. It only stays in the test phase, in the laboratory. So we usually just focus on the test side. But we do usually create a list of operational issues that we know will be coming up, and so we try to give those issues to the operational component privacy officers and give them a heads-up as to what to expect and suggestions on how to address those issues.

MS. CALLAHAN: Joanne, this is Mary Ellen Callahan, the Privacy Officer.

CHAIRMAN PURCELL: We knew.

MS. CALLAHAN: Well, just in case the court reporter didn't know.

Science and Technology sometimes will acknowledge that, as Chris pointed out, here in testing the privacy risk is mitigated for the following reasons; in an operational capacity there may be additional privacy risks, and that would be further developed in an operational Privacy Impact Assessment.

But I think having Chris and Kathryn and Jaeme identify the potential areas certainly helps give a leg up when we transition from a testing Privacy Impact Assessment to an operational Privacy Impact Assessment.

And my office, primarily Director of Privacy Compliance Becky Richards and her staff, work together to make sure that we are again dealing with the life cycle of the policy and the program and that the privacy assessments are addressed at each stage.

Ms. McNABB: One other question. I don't know, Christopher, if you've looked at a document that this committee presented several years ago called "A Framework for Assessing the Privacy Impacts of Programs and Technologies." It's on the web site on the privacy page and on the committee page.

It starts at the beginning of determining what is the threat that this program or technology is designed to meet and works through a real basic risk management process before the privacy issues even come up.

Do you at all approach programs in S&T in that way?

MR. LEE: I do approach the programs in terms of risk-benefit analysis, in terms of what is the risk, what are they trying to solve, and what's the benefit if we are able to solve that analysis. So we do go through these balancing tests to identify what the risks are and try to

mitigate those risks.

Ms. McNABB: Thank you. That doesn't always come out in the Privacy Impact Assessment and your Privacy Impact Assessment tool isn't necessarily designed to present that. But I think it would be useful to address that in a PIA.

MR. LEE: I think having that balancing test would be helpful to everybody, yes.

CHAIRMAN PURCELL: Thank you, Joanne.

Are there other members with questions, please? Identify yourself.

(No response.)

CHAIRMAN PURCELL: I hear no further questions. Mr. Lee, thank you very much for your comments today. I appreciate that.

MR. LEE: Thank you, Mr. Chairman.

CHAIRMAN PURCELL: I'd like to turn now to Mary Ellen Callahan, our Chief Privacy Officer. She has some remarks she'd like to make.

MS. CALLAHAN: Great. Thank you, Richard.

I just want to thank everyone for participating in this experiment. I think we've got some lessons

learned if we do another call, but I appreciate everyone's indulgence on this.

I wanted to make a few kind of closing remarks, so I asked the Chairman for the floor one more time. I just wanted to kind of acknowledge that this is a little bit of a transition period, both for the Privacy Office with regard to DPIAC as well as for some of the DPIAC members as well. Just for the members' awareness, the first assistant I think for DPIAC, Tamara Baker, has actually moved on to the USCIS Privacy Office. So she is now supporting Donald Hawkins, who of course appeared before the committee last year -- last time, excuse me, in March.

I wanted to publicly thank Tamara for all of her hard work on DPIAC and on everything else that she has worked on. We ended up figuring out that, other than Pete and Becky, Tamara was the longest-standing employee for the Privacy Office. So we want to thank her, and I know that you guys knew her well in her different roles supporting DPIAC and then in Compliance.

Christal Hoo has also moved on, but has stayed in the family, and she has moved to help support Latita

Payne at the U.S. Secret Service. So those are the kind of transitions in the Privacy Office. And Bill Holzerland and Vania Lockett have each moved on, Bill to become the first FOIA officer at the Consumer Financial Protection Bureau and Vania to support Emily Andrew at NPPD, so she again stays in the family, moves from FOIA, but to Privacy. So our community is getting more diverse and broader, but we want to congratulate all of them.

Speaking of transitions, this will be the last DPIAC committee meeting for several of our very longstanding and supportive members of the DPIAC. It's a somewhat bittersweet moment as we bid farewell to these members. I wanted to publicly thank them for their support of DPIAC and helping us on many, a variety of different issues.

Jim Harper and Kirk Herath have served on the committee since January 2005. They were both appointed as original members of the committee. Larry Ponemon and Neville Pattinson were appointed by the committee the next year in August 2006; and Dan Caprio first joined the committee in July of 2007. All five, this will be their last participation in the DPIAC as a member, but I hope

that they continue to join and to be part of the extended DHS community throughout their careers.

The Department is really indebted to all of you. During your tenure the committee has made significant contributions to the Department through its independent substantial advice on a wide range of issues. Joanne mentioned one, but let me also identify several others where we received stalwart guidance on privacy issues, including: the Department's use of commercial data -- that continues to be a signature piece, and that we point to throughout the Federal Government; the Secure Flight and E-Verify programs and their related improvements as a result of the DPIAC's contribution; the Department's information-sharing agreements with external organizations; and the elements of effective privacy redress programs, both of which are being implemented by the Department and have made a difference on a daily basis.

I wanted to publicly thank the five departing members, and I trust you will continue to follow the committee's work and to contribute to the ongoing public dialogue as we work to build an even stronger privacy

program at DHS.

The Secretary has written to all five members to say thank-you for their ongoing support. I want to add my thanks to those of the Secretary. We are grateful for your service and the committee is better as a result of it.

The committee will next meet in July, likely July 11th, and at that time we will be announcing a new slate of DPIAC members and they will be officially introduced at that event. We look forward to their hard work, energy, and novel approaches to privacy protection and we look forward to continuing the work of the DPIAC with both returning and new members aboard.

Thank you, Mr. Chairman.

CHAIRMAN PURCELL: Thank you, Mary Ellen. I appreciate that.

I'd like to just take a short moment to express my own thanks to Dan, to Larry, to Jim, to Neville, and to Kirk. Each of these individuals has dedicated a large part of their time to this committee. They've contributed quite a lot of intellectual and working capital to the committee's work, perhaps the most unique being Jim

Harper. I think "unique" is an understatement. Tough to replace that act.

But nonetheless, Dan, Larry, Jim, Neville, Kirk have all been hard-working, contributing, and valuable members whose efforts to the committee have been deeply appreciated and will be missed. We look forward to continuing our long-time relationships with these individuals as privacy professionals and concerned citizens. So my sincere thanks for their service to this committee.

PUBLIC COMMENTS

CHAIRMAN PURCELL: This is the moment now where we take public comments. So first I want to thank Mary Ellen and Christopher Lee for the report they've provided us this morning. I'd like also to remind any members of the public that if they would like to address the committee they're able to at this time, if they would state their name and affiliation, if any. A reminder that these remarks are limited to 3 minutes so that others may speak as well.

So if there's anyone here, members of the public, who would like to make a statement or a comment to

the committee, please state your name at this time.

(No response.)

CHAIRMAN PURCELL: Hearing none, I will remind the members of the public that they may submit comments to the committee at any time by emailing them to the email address privacycommittee@dhs.gov. That's on the web site.

I want to express my sincere thanks to our speakers and all of you for attending this meeting this morning, and this concludes the public portion of today's meeting. We're grateful for the interest you've shown in the committee's work.

The transcript and minutes of this meeting will be posted on the DHS Privacy Office's web site at dhs.gov/privacy as soon as we're able to post them, and we encourage you to follow the committee's work by checking our web page frequently.

Thank you all for your participation. This draws our meeting to a close.

(Whereupon, at 12:05 p.m., the meeting was adjourned.)